



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/539,648

12/17/2007

John Owlett

GB920020055US1

6660

30449 7590 02/17/2010
SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER

WOLDEMARIAM, NEGA

ART UNIT

PAPER NUMBER

2433

MAIL DATE

DELIVERY MODE

02/17/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/539,648	Applicant(s) OWLETT ET AL.	
	Examiner NEGA WOLDEMARIAM	Art Unit 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 November 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 27-49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 27-49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>09/29/2009</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to application filed on the 12th of November 2009.
2. Claims 1 and 27—49 are currently pending. Claims 2—26 are canceled.
3. The IDS submitted on 09/29/2009 is accepted
4. The 35 U.S.C 101 rejection is removed due to applicant amendment.

Response to Amendment

Applicant's arguments filed on the 12th of November 2009 have been fully considered; however, they are moot in view of the new ground of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, and 27—49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi et al. US Publication No.: 7099846 B1(hereinafter Ishibashi) and in view of Sudia et al. US Patent. No.: 5995625 (hereinafter Sudia) (please refer to

As to claim 1, Ishibashi teaches **a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item), **the method comprising: the data item to generate a digest of the data item** (see Ishibashi col. 15 lines 5—7, generating

Art Unit: 2433

message/data digest); **hashing each condition of the one or more conditions separately from each other and separately from the data item, mad to generate one or more condition digests respectively corresponding to the one or more conditions** (see Ishibashi col. 23 lines 20—25 and Fig 26 each record/data item has separate condition signature and it is separate from the data item); **setting a reference digest equal to the digest of the data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item); Ishibashi does not explicitly teach the following, **a computer iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests**, however Sudia teaches (see Fig. 1, and col. 7 lines 30—35 unique conditions, acceptance phrase and optionally other data can first be combined and then their combination can be digested repeatedly/iteratively) , **said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed** (see Sudia Fig. 2, Fig. 8 and col. 8 line 55—59, a hash of the acceptance phrase/condition is combined/concatenated with a hash of the issuing policy statement/condition repeatedly with other key information such as random value to form key value) , **each unique condition digest being a different condition digest in each iteration of the loop** (se Sudia col. 5 lines 13—26 , multiple condition, acceptance phrase and data may be different and create unique digest and the process repeat itself) , **the regenerated reference digest of the last iteration of the loop being last digest** (see Sudia col. 19 lines 57—67, wrapped signature/digest condition, product or data be wrapped creating a series of wrapped

Art Unit: 2433

data); **and encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the current invention to combine the teachings of Ishibashi and Sudia to create the invention as claimed. The teachings are all directed to digital content and access condition hashing, encryption and digital signature, as is the current application – therefore, the teachings are in an analogous art. Further, it would have been obvious to one of ordinary skill in the art that using iteration combining/concatenating the hashed conditions until encrypting the last digest with a digital signature. It would have been clear to one of ordinary skill in the art that iteratively wrapping the hashed conditions and encrypting the wrap with digital signature increases security and integrity.

As to 27, the combination of Ishibashi and Sudia teaches **the method, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions** (see Sudia col. 2 lines 61—65, a particular pass phrase indicating acceptance of conditions of digital data)

As to 28, the combination of Ishibashi and Sudia teaches **the method, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions** (see Sudia col. 8 lines 32—42 the subscriber accept and digitally sign acceptance of conditions)

As to 29, the combination of Ishibashi and Sudia teaches **the method, said method further comprising: generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and sending the communication across a network to a recipient** (see Sudia col. 19, lines 37—46, sending wrapped digital data and conditions over a network including digital signature)

As to 30, the combination of Ishibashi and Sudia teaches **the method, said method further comprising: generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and sending the communication across a network to a recipient** (see Sudia col. 12, lines 1—7, key value digital signature is sent to verify the wrapped content and condition)

As to 31, the combination of Ishibashi and Sudia teaches **the method, wherein the method further comprises: hashing a new condition to generate a digest of the new condition; concatenating the digital signature block with the digest of the new condition to generate a new digest; hashing the new digest to generate a hashed new digest; and encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to 32, the combination of Ishibashi and Sudia teaches **the method, wherein the one or more conditions consists of one condition** (se Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to 33, the combination of Ishibashi and Sudia teaches **the method, wherein the one or more conditions is a plurality of conditions** (se Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 34, Ishibashi teaches **a computer program product, comprising a machine-readable recording medium having program code recorded thereon, said program code upon being executed by a data processing apparatus causes the data processing apparatus to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item), **said method comprising: hashing the data item to generate a digest of the data item; hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions** (see Ishibashi col. 23 lines 20—25 and Fig 26 each record/data item has separate condition signature and it is separate from the data item); **setting a reference digest equal to the digest of the data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item); **a data processing apparatus iteratively processing a unique**

Art Unit: 2433

condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests however Sudia teaches (see Fig. 1, and col. 7 lines 30—35 unique conditions, acceptance phrase and optionally other data can first be combined and then their combination can be digested repeatedly/iteratively), **said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed** (see Sudia Fig. 2, Fig. 8 and col. 8 line 55—59, a hash of the acceptance phrase/condition is combined/concatenated with a hash of the issuing policy statement/condition repeatedly with other key information such as random value to form key value), **each unique condition digest being a different condition digest in each iteration of the loop** (see Sudia col. 5 lines 13—26, multiple condition, acceptance phrase and data may be different and create unique digest and the process repeat itself), **the regenerated reference digest of the last iteration of the loop being a last digest** (see Sudia col. 19 lines 57—67, wrapped signature/digest condition, product or data be wrapped creating a series of wrapped data); **and encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the current invention to combine the teachings of Ishibashi and Sudia to create the invention as claimed. The teachings are all directed to digital content and access condition hashing, encryption and digital signature, as is the current application – therefore, the teachings are in an analogous art. Further, it would have been obvious to one of ordinary skill in the art that using iteration combining/concatenating the hashed conditions until encrypting the last digest with a digital signature. It would have been clear to one of ordinary skill in the art that iteratively wrapping the hashed conditions and encrypting the wrap with digital signature increases security and integrity.

As to claim 35, the combination of Ishibashi and Sudia teaches **the computer program product, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions** (see Sudia col. 2 lines 61—65, a particular pass phrase indicating acceptance of conditions of digital data)

As to claim 36, the combination of Ishibashi and Sudia teaches **the computer program product, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions** (see Sudia col. 8 lines 32—42 the subscriber accept and digitally sign acceptance of conditions)

As to claim 37, the combination of Ishibashi and Sudia teaches **the computer program product, said method further comprising: generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more**

Art Unit: 2433

conditions; and sending the communication across a network to a recipient (see Sudia col. 19, lines 37—46, sending wrapped digital data and conditions over a network including digital signature)

As to claim 38, the combination of Ishibashi and Sudia teaches **the computer program product, said method further comprising: generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and sending the communication across a network to a recipient** (see Sudia col. 12, lines 1—7, key value digital signature is sent to verify the wrapped content and condition)

As to claim 39, the combination of Ishibashi and Sudia teaches **the computer program product, wherein the method further comprises: hashing a new condition to generate a digest of the new condition; concatenating the digital signature block with the digest of the new condition to generate a new digest; hashing the new digest to generate a hashed new digest; and encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 40, the combination of Ishibashi and Sudia teaches **the computer program product, wherein the one or more conditions consists of one condition** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 41, the combination of Ishibashi and Sudia teaches **the computer program product, wherein the one or more conditions is a plurality of conditions** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 42, Ishibashi teaches **a data processing apparatus comprising a computer and a machine-readable recording medium coupled to the computer, said recording medium storing program code that when executed by the computer causes the computer to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item), **said method comprising: hashing the data item to generate a digest of the data item** (see Ishibashi col. 15 lines 5—7, generating message/data digest); **hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions** (see Ishibashi col. 23 lines 20—25 and Fig. 26 each record/data item has separate condition signature and it is separate from the data item); **setting a reference digest equal to the digest of the data item** (see Ishibashi col. 23 lines 20—25 and Fig. 26, electronic signatures stored for conditions to the information/data item); Ishibashi does not explicitly teach

Art Unit: 2433

the following, **a data processing apparatus iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests** however Sudia teaches (see Fig. 1, and col. 7 lines 30—35 unique conditions, acceptance phrase and optionally other data can first be combined and then their combination can be digested repeatedly/iteratively), **said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed** (see Sudia Fig. 2, Fig. 8 and col. 8 line 55—59, a hash of the acceptance phrase/condition is combined/concatenated with a hash of the issuing policy statement/condition repeatedly with other key information such as random value to form key value), **each unique condition digest being a different condition digest in each iteration of the loop** (see Sudia col. 5 lines 13—26, multiple condition, acceptance phrase and data may be different and create unique digest and the process repeat itself), **the regenerated reference digest of the last iteration of the loop being a last digest** (see Sudia col. 19 lines 57—67, wrapped signature/digest condition, product or data be wrapped creating a series of wrapped data); **and encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the current invention to combine the teachings of Ishibashi and Sudia to create the invention as claimed. The teachings are all directed to digital content and access condition hashing, encryption and digital signature, as is the current application – therefore, the teachings are in an analogous art. Further, it would have been obvious to one of ordinary skill in the art that using iteration combining/concatenating the hashed conditions until encrypting the last digest with a digital signature. It would have been clear to one of ordinary skill in the art that iteratively wrapping the hashed conditions and encrypting the wrap with digital signature increases security and integrity.

As to claim 43, the combination of Ishibashi and Sudia teaches **the data processing apparatus, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions** (see Sudia col. 2 lines 61—65, a particular pass phrase indicating acceptance of conditions of digital data)

As to claim 44, the combination of Ishibashi and Sudia teaches **the data processing apparatus, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions** (see Sudia col. 8 lines 32—42 the subscriber accept and digitally sign acceptance of conditions)

As to claim 45, the combination of Ishibashi and Sudia teaches **the data processing apparatus, said method further comprising: generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and sending the communication across a network to a recipient** (see Sudia col.

Art Unit: 2433

19, lines 37—46, sending wrapped digital data and conditions over a network including digital signature)

As to claim 46, the combination of Ishibashi and Sudia teaches **the data processing apparatus, said method further comprising: generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and sending the communication across a network to a recipient** (see Sudia col. 12, lines 1—7, key value digital signature is sent to verify the wrapped content and condition)

As to claim 47, the combination of Ishibashi and Sudia teaches **the data processing apparatus, wherein the method further comprises: hashing a new condition to generate a digest of the new condition; concatenating the digital signature block with the digest of the new condition to generate a new digest; hashing the new digest to generate a hashed new digest; and encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 48, the combination of Ishibashi and Sudia teaches **the data processing apparatus, wherein the one or more conditions consists of one condition** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

As to claim 49, the combination of Ishibashi and Sudia teaches **the data processing apparatus, wherein the one or more conditions is a plurality of conditions** (see Sudia Fig. 8 and col. 11 lines 45—64, multiple condition, acceptance phrase and data may be wrapped combined hashed and encrypted)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **NEGA WOLDEMARIAM** whose telephone number is (571)270-7478. The examiner can normally be reached From Monday to Friday between the hours of 8:00am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kieu-Oanh (Krista) Bui can be reached on 571-272-7291. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KIEU-OANH BUI/
Supervisory Patent Examiner, TC 2400

NEGA WOLDEMARIAM
Examiner, Art Unit 2433